

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION
CASE NO. 3:19-CV-643-RJC-DCK**

SENSORRX, INC.,

Plaintiff,

v.

ELI LILLY AND COMPANY,

Defendant.

)
)
)
)
)
)
)
)
)
)
)

ESI CONSENT ORDER

WHEREAS, counsel for Plaintiff SensorRx and Defendant Eli Lilly and Company (collectively, the “Parties,” and each, a “Party”) have met and conferred regarding discovery of electronically stored information (“ESI”) of the Parties;

WHEREAS, the Parties have reached agreement on certain issues discussed regarding such discovery and filed a “Joint Motion For Entry Of ESI Consent Order” (Document No. 74);

WHEREAS, the Parties have agreed upon this ESI Consent Order concerning protocol for production of electronically stored information (“ESI Order”) to facilitate the just, speedy, and inexpensive conduct of discovery involving ESI and to promote, to the fullest extent possible, the resolution of disputes regarding the discovery of ESI without Court intervention;

IT IS HEREBY ORDERED that:

1. All Parties are bound by and subject to the terms of this Order.
2. The Parties agree to meet and confer as to each Party's data sources most likely to contain relevant information, discovery sequencing, search parameters, and cost considerations after both sides have served initial sets of written discovery. Upon completion of the meet and confer, the Parties will promptly raise any unresolved issues with the Court via Joint Status Report.

3. Definitions.

a. “Documents” and “Electronically Stored Information” (“ESI”) shall be defined as they are in Federal Rule of Civil Procedure 34.

b. “Discovery Material” is defined as all products of discovery and all information derived therefrom, including, but not limited to, documents, objects and things, deposition testimony, interrogatory/request for admission responses, and any copies, excerpts or summaries thereof, produced by any Party in the above-captioned matter.

c. “Protective Order” shall refer to the stipulated protective order that the Parties agree to and is entered by the Court, including any amendments thereto.

d. Plaintiff and Defendant, as well as their officers, directors, employees, agents, and legal counsel, are referred to as the “Parties” solely for the purposes of this Protocol.

4. Cooperation. The Parties shall conduct discovery in a cooperative manner, including without limitation, by drafting reasonable discovery requests and responses in accordance with Federal Rule of Civil Procedure 1 and 26(g)(1); and producing ESI in accordance with Federal Rule of Civil Procedure 34; and by meeting and conferring in good faith on any issue regarding ESI, as necessary, that may arise during the course of discovery.

5. Proportionality. The proportionality standard set forth in Federal Rule of Civil Procedure 26(b)(1) shall be applied in all matters related to discovery of ESI, including without limitation the preservation, collection, and production of such information. To further the application of the proportionality standard, requests for production of ESI and related responses shall be reasonably targeted, clear, and as specific as practicable.

6. ESI Liaisons. The ESI Liaisons for Plaintiff shall be John Martin, Heyward Bonyata, and Michael Bigham of the law firm of Nelson Mullins Riley & Scarborough LLP. The

ESI Liaison for Defendant shall be Jeremy Williams of the law firm Whitfield Bryson, LLP. The Parties agree to work in good faith to schedule e-discovery conferences when the ESI Liaisons are available.

7. Data Sources and Search Methodology.

a. The Producing Party shall be responsible for a good-faith collection, review, and production of ESI responsive to any appropriate discovery request. The production of discovery materials, including ESI, and any related disagreements between the Parties related to the scope or manner of production of ESI, shall be governed by the Federal Rules of Civil Procedure, local rules of the Court, or Order of the Court.

b. The Parties agree that there is no need to collect the following ESI :

- i. ESI deleted as a result of the routine, good-faith operation of an ESI system;
- ii. Unallocated data, slack space, deleted data, file fragments or other data accessible only by use of computer forensics;
- iii. Random access memory (RAM) or other ephemeral data.
- iv. Online access data such as temporary internet files, histories, caches, cookies, etc.
- v. Data contained in disaster recovery systems and retention backup tapes, except as specified herein
- vi. Data in metadata fields frequently updated automatically as part of the usual operation of a software application, such as last-opened or last-printed dates;

- vii. Telephone voice messages unless they are transcribed in the ordinary course;
- viii. Operating system files, executable files, network, server, software application or system logs;
- ix. Files on the NIST list; and
- x. Legacy data from systems or software applications no longer in use when such data cannot be read or interpreted by systems or software applications currently in use.

The parties agree to meet and confer regarding the production of ESI from the above categories should discovery reveal that responsive information exists in one or more of these categories.

c. All meet and confer sessions under this paragraph will involve one of each Party's respective e-discovery liaisons, unless the parties agree otherwise, and will give appropriate consideration to minimizing expense.

8. E-mail Threading. In order to reduce the volume of entirely duplicative content within e-mail threads, the Parties may utilize "e-mail thread suppression." As used in this Order, e-mail thread suppression means reducing duplicative production of e-mail threads by producing comprehensive e-mails containing the thread of e-mails and excluding e-mails constituting exact duplicates of e-mails within the produced string. Duplicative e-mails suppressed under this paragraph need not be reflected on the Party's privilege log, as further discussed in paragraph 9.

9. Privileged Information. This Order does not address the Parties obligations with respect to privileged information. Provisions regarding the timing of, exchange of, and other

parameters for the Parties' privilege logs, along with procedures regarding the production of privileged material, will be located in the Protective Order.

10. Metadata. The following metadata fields will be produced for each document to the extent that such information is available at the time of collection and processing:

- a. BEGINDOC
- b. ENDDOC
- c. BEGATTACH
- d. ENDATTACH
- e. SOURCE / CUSTODIAN
- f. FILEEXTENSION
- g. FILENAME
- h. FILEPATH
- i. DOCDATE
- j. AUTHOR
- k. TO
- l. FROM
- m. CC
- n. BCC
- o. SUBJECT
- p. CONFIDENTIALITY

This list of fields does not create any obligation to create or manually code fields that are not automatically generated by the processing of ESI, that do not exist as part of the original metadata of the document, or would be burdensome or costly to obtain as set forth in Rule 26(b) of the Federal Rules of Civil Procedure.

11. Production Format. All documents, unless otherwise specified in Paragraph 11.a. below, whether stored as paper or ESI, will be produced by both Parties as black-and-white, where the original document is black and white, and in color where the original document is in color.

Black and white documents shall be produced as single-page, 300 dpi (minimum) Group IV TIFF images or single-page JPG images, and color documents shall be produced as single page .JPG images. All documents, whether black and white or in color, shall be OCR searchable, with text in document level text files, with a load file that references the images and text, and a .DAT file with delimiters that list the metadata fields below. The UTF-8 character set should be used for all extracted/OCR text files in a production. Image reference load files will be provided in .OPT format. After production in this format is received, the Parties will meet and confer regarding any good faith request for the production of ESI in native file format.

a. Native Format. The Parties shall produce Excel spreadsheets (and their reasonable equivalent), audio files, and video files in native format, unless redacted, with extracted searchable text and the applicable metadata specified in this ESI Order.

b. Parent-Child Relationships. Parent-child relationships (the association between e-mails and attachments) will be preserved. E-mail attachments will be consecutively produced with the parent e-mail record. If an e-mail attachment is privileged, not responsive, or has a technical issue, a slip sheet shall be inserted in the production noting the reason for the slip sheet.

c. Dynamic Fields. Documents with dynamic fields for file names, dates, and times will be processed to show the field code (e.g., “[FILENAME]” or “[AUTODATE]”), rather than the values for such fields existing at the time the file is processed.

d. Database Records. To the extent that any Party requests information that is stored in a database or database management system, the Parties will meet and confer regarding the accessibility of such information and the format of production.

e. Non-Traditional Data Sources or Files. Non-traditional data sources or files include, but are not limited to, transactional data, structured databases, database files, audio and video files, and proprietary applications not publicly available. Upon request and demonstration of need, the Parties will meet and confer as to a reasonable production format for such files.

f. Time Zone. Unless otherwise agreed, all dynamic date and time fields, where such fields are processed to contain a value, and all metadata pertaining to dates and times will be standardized to Eastern Time. The Parties understand and acknowledge that such standardization affects only dynamic fields and metadata values and does not affect, among other things, dates and times that are hardcoded text within a file. Dates and times that are hard-coded text within a file (for example, in an e-mail thread, dates and times of earlier messages that were converted to body text when subsequently replied to or forwarded; and in any file type, dates and times that are typed as such by users) will be produced as part of the document text in accordance with the load file formats, below.

g. Bates Numbering. Files will be named according to the Bates number of the corresponding *.tiff image. The Bates number will:

- i. be consistent across the production;
- ii. contain no special characters; and
- iii. be numerically sequential within a given document.

Attachments to documents will be assigned Bates numbers that directly follow the Bates numbers on the documents to which they were attached. If a Bates number or set of Bates numbers is skipped, the skipped number or set of numbers will be noted. In addition, wherever possible, each *.tiff image will have its assigned Bates number electronically “burned” onto the image.

h. Other Branding. In addition, to the extent any image or file is to be marked “confidential” pursuant to the terms of the Protective Order, each page of the image or file to be so marked shall include the appropriate confidentiality designation. If a native file is produced, the Party producing such native file shall include a single-image placeholder TIFF with a single Bates number on the image itself. The native file will be linked to the placeholder TIFF and the Bates number assigned thereto. There shall be no Bates numbering of native files at the page level. To the extent the producing Party designates a native file as confidential pursuant to the terms of the Protective Order, the placeholder TIFF shall be so designated.

i. Production Media. The producing Party may produce documents via a secure file transfer mechanism and/or on readily accessible, computer or electronic media. Each piece of Production Media will be assigned a production number or other unique identifying label corresponding to the date of the production as well as the sequence of the material in that production.

12. Encryption. To maximize the security of information in transit, any media on which documents are produced may be encrypted by the producing Party. In such cases, the producing Party shall transmit the encryption key or password to the requesting Party, under separate cover, contemporaneously with sending the encrypted media.

13. Authenticity and Admissibility. Nothing in this protocol shall be construed to affect the authenticity or admissibility of any document or data. All objections to the authenticity or admissibility of any document or data are preserved and may be asserted at any time.

14. Confidentiality or Highly Confidential Attorneys’-Eyes-Only Information. For the avoidance of doubt, nothing herein shall contradict the Parties’ rights and obligations with respect

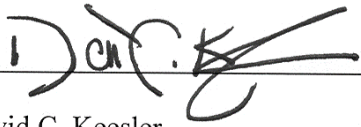
to any document or data designated as confidential, as governed by the Protective Order regarding the protection of such information.

15. Preservation. The parties agree to take reasonable steps to preserve ESI relevant to the Parties' claims and defenses.

16. Claw Back Agreement. See Paragraph IX of the Stipulated Protective Order.

SO ORDERED.

Signed: January 22, 2021



David C. Keesler
United States Magistrate Judge

